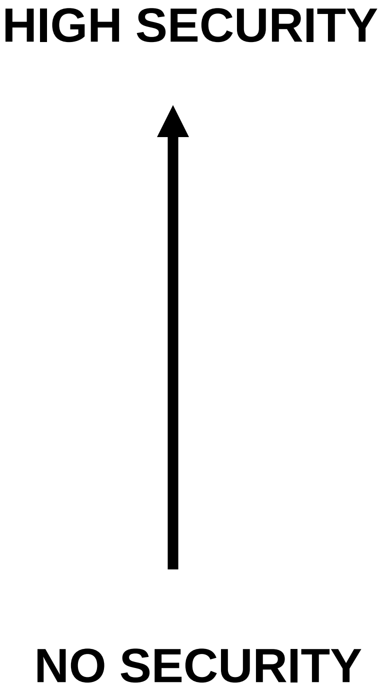
THE ORANGE BOOK

Ravi Sandhu

ORANGE BOOK CLASSES



HIGH SECURITY

NO SECURITY

A1	Verified Design
B3	Security Domains
B2	Structured Protection
B1	Labeled Security Protection
C2	Controlled Access Protection
C1	Discretionary Security Protection
D	Minimal Protection

ORANGE BOOK CRITERIA

SECURITY POLICY

ACCOUNTABILITY

ASSURANCE

DOCUMENTATION

SECURITY POLICY

	C1	C2	B1	B2	B3	A1
Discretionary Access Control	+	+	nc	nc	+	nc
Object Reuse	0	+	nc	nc	nc	nc
Labels	0	0	+	+	nc	nc
Label Integrity	0	0	+	nc	nc	nc
Exportation of Labeled Information	0	0	+	nc	nc	nc
Labeling Human-Readable Output	0	0	+	nc	nc	nc
Mandatory Access Control	0	0	+	+	nc	nc
Subject Sensitivity Labels	0	0	0	+	nc	nc
Device Labels	0	0	0	+	nc	nc

0	no requirement
+	added requirement
nc	no change

ACCOUNTABILITY

	C1	C2	B1	B2	B3	A1
Identification and Authentication	+	+	+	nc	nc	nc
Audit	0	+	+	+	+	nc
Trusted Path	0	0	0	+	+	nc

0	no requirement
+	added requirement
nc	no change

ASSURANCE

	C1	C2	B1	B2	B3	A1
System Architecture	+	+	+	+	+	nc
System Integrity	+	nc	nc	nc	nc	nc
Security Testing	+	+	+	+	+	+
Design Specification and Verification	0	0	+	+	+	+
Covert Channel Analysis	0	0	0	+	+	+
Trusted Facility Management	0	0	0	+	+	nc
Configuration Management	0	0	0	+	nc	+
Trusted Recovery	0	0	0	0	+	nc
Trusted Distribution	0	0	0	0	0	+

0	no requirement
+	added requirement
nc	no change

DOCUMENTATION

	C1	C2	B1	B2	B3	A1
Security Features User's Guide	+	nc	nc	nc	nc	nc
Trusted Facility Manual	+	+	+	+	+	nc
Test Documentation	+	nc	nc	+	nc	+
Design Documentation	+	nc	+	+	+	+

0	no requirement
+	added requirement
nc	no change

COVERT CHANNEL ANALYSIS

B1	No requirement
B2	Covert storage channels
B3	Covert channels (i.e. storage and timing channels)
A1	Formal methods

SYSTEM ARCHITECTURE

C1 The TCB shall maintain a domain for its own execution that protects it from tampering

C2 The TCB shall isolate the resources to be protected

B1 The TCB shall maintain process isolation

B2 The TCB shall be internally structured into well-defined largely independent modules

B3 The TCB shall incorporate significant use of layering, abstraction and data hiding

A1 No change

DESIGN SPECIFICATION AND VERIFICATION

C2 No requirement

B1 Informal or formal model of the security policy

B2 Formal model of the security policy that is proven consistent with its axioms

DTLS (descriptive top-level specification) of the TCB

B3 A convincing argument shall be given that the DTLS is consistent with the model

A1 FTLS (formal top-level specification) of the TCB

A combination of formal and informal techniques shall be used to show that the FTLS is consistent with the model

A convincing argument shall be given that the DTLS is consistent with the model

ORANGE BOOK CLASSES UNOFFICIAL VIEW

C1, C2 Simple enhancement of existing systems. No breakage of applications

B1 Relatively simple enhancement of existing systems. Will break some applications.

B2 Relatively major enhancement of existing systems. Will break many applications.

B3 Failed A1

A1 Top down design and implementation of a new system from scratch

NCSC RAINBOW SERIES SELECTED TITLES

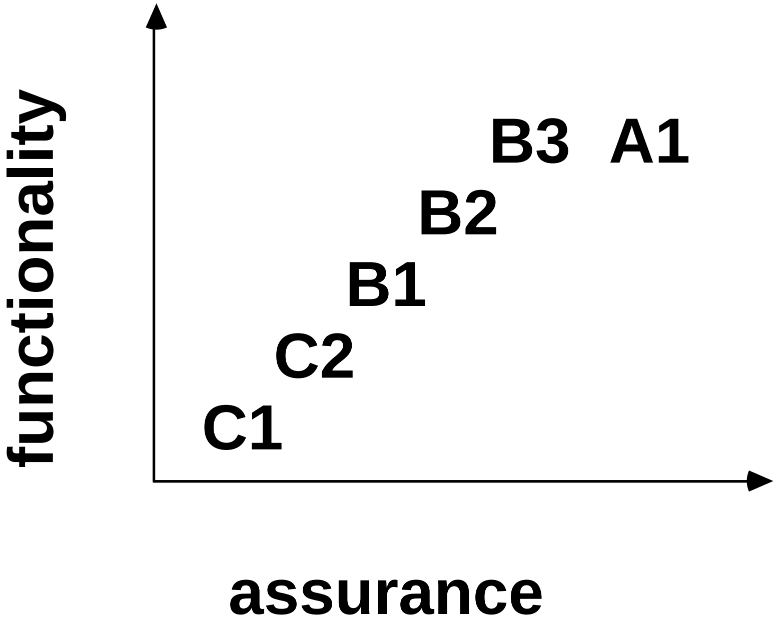
Orange	**Trusted Computer System Evaluation Criteria**
Yellow	**Guidance for Applying the Orange Book**
Red	**Trusted Network Interpretation**
Lavender	**Trusted Database Interpretation**

ORANGE BOOK CRITICISMS

- Mixes various levels of abstraction in a single document
- Does not address integrity of data
- Combines functionality and assurance in a single linear rating scale

FUNCTIONALITY VS ASSURANCE

- functionality is multi-dimensional
- assurance has a linear progression


functionality
B3
A1
B2
B1
C2
C1
assurance